A24

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/489,696	01/24/2000	Shigeo Tsujii	FORM PTO-1082	6150

26021 7590 02/12/2004

HOGAN & HARTSON L.L.P.
500 S. GRAND AVENUE
SUITE 1900
LOS ANGELES, CA 90071-2611

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2135	6

DATE MAILED: 02/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

ppg

Office Action Summary	**Application No.** 09/489,696	**Applicant(s)** TSUJII ET AL.
	Examiner Thanhnga Truong	**Art Unit** 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 24 January 2000 .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-23 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-23 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 24 January 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 3 and 5 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-4, 7-13, and 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Baba (US 5,987, 129).

a. Referring to claim 1:

i. Baba teaches:

(1) generating said secret keys peculiar to said entities using pieces of' information resulting from division of information specifying each of said entities **[i.e., generating, in the center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by the center only and common to the entities and which includes at least an integral transformation algorithm, and distributing, from the center, the secret private key and the integral transformation algorithm to each of the entities (column 2, lines 50-57)]**.

b. Referring to claim 2:

i. Baba teaches:

(1) generating said secret keys peculiar to said entities using pieces of' information resulting from division of information specifying each of said entities **[i.e., generating, in the center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by the center only**

and common to the entities and which includes at least an integral transformation algorithm, and distributing, from the center, the secret private key and the integral transformation algorithm to each of the entities (column 2, lines 50-57)]; and

(2) encrypting plaintext to ciphertext using a common key generated using a component contained in the secret key peculiar to an entity that is a sender of the ciphertext, the component corresponding to one or more pieces of information specifying another entity that is a destination of the ciphertext **[i.e., Figure 6 clearly shows the process of "encrypting plaintext to ciphertext using a common key generated using a component contained in the secret key peculiar to an entity that is a sender of the ciphertext, the component corresponding to one or more pieces of information specifying another entity that is a destination of the ciphertext" (column 10, lines 30-40 and column 11, lines 32-50)].**

c. *Referring to claim 3:*

i. Baba teaches:

(1) a cryptographic, communications method for communications of information between entities wherein a plurality of centers are provided, each of which generates secret keys peculiar to the entities using divided pieces of information resulting from division of information specifying each of the entities; one entity generates a first common key using a first component contained in secret keys peculiar to the one entity sent from the centers, encrypts plaintext to ciphertext using the first common key and sends the ciphertext to another entity, the first component corresponding to one or more of the divided pieces of information specifying said another entity; and said another entity generates a second common key identical to the first common key using a second component contained in secret keys peculiar to the another entity sent from said centers, and decrypts said ciphertext to the original plaintext using the second common key, the second component corresponding to one or more of the divided pieces of information specifying the one entity **[i.e., as shown in Figure 1, a the cryptosystem includes a center or central facility 1, which is a basic main constituent of the system, a plurality of entities 2 which are**

subscribed to the cryptosystem for communication with each other, and a network 3 such as the Internet, a personal computer communication network, or the like through which the center 1 and the entities 2 are connected to communicate with each other. The center 1 and the entities 2 include computers such as personal computers for effecting actual communications and data processing and users of those computers. In the cryptosystem on the network 3, as shown in Figure 2, the entities 2 (represented by i, j, . . . in Figure 2) have respective peculiar identifiers yi, yj, . . . (described in detail later on). If i.noteq.j, then yi.noteq.yj. The entities 2 (i, j, . . .) have been given, by the center 1, respective secret private keys Xi, Xj, . . . (described in detail later on and hereinafter referred to as a "secret private key Xn" if necessary) which are peculiar to the respective entities 2 and generated by the center 1 based on the respective identifiers yi, yj, . . . (hereinafter referred to as an "identifier yn" if necessary). For cryptographic communications between any arbitrary entities i, j, a common cryptokey Kij for encrypting communication data (on the transmitting side) and decrypting communication data (on the receiving side) is generated for the entities i, j using the secrete private keys Xi, Xj of the entities i, j. Using the generated common cryptokey Kij, the encrypted communications are carried out between the entities i, j. The cryptosystem for carrying out the above cryptographic communications described in detail with reference to Figures 3 through 8 (column 8, lines 66-67 through column 12, lines 34)]. In addition, if there are a plurality of centers, then "xi" in the equation Vi(.eta.)=xi.multidot.f.eta.is replaced with the summation of the matrix xi determined as described above for each of the centers (column 16, lines 8-10)].

d. *Referring to claim 4:*

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

e. *Referring to claim 7:*

i. Baba teaches:

(1) storage means at each entity for storing secret keys peculiar to each respective entity produced for respective pieces of information resulting from division of information specifying each of said respective entities **[i.e., referring to Figure 1, When each entity 2 receives the secret private key Xn and the identifier transformation algorithm, it stores them secretly in a suitable storage device of its own computer (column 10, lines 14-16)];**

(2) selection means for selecting components corresponding to pieces of information specifying opposite entities to be communicated with, from among the secret keys stored; and means for generating said common keys using said components so selected **[i.e., in the cryptosystem, the secret private key of each entity 2 is generated and a common cryptokey is generated according to a linear transformation or scheme. It is assumed that Xif represents the secret private key of an entity i for the generation of a common cryptokey shared by f entities 2. According to a general concept for constructing the above linear scheme, that is "selection", an f-input symmetric transformation g (which is a symmetric function having f variables) is arbitrarily selected (column 15, lines 12-20)].**

f. <u>*Referring to claim 8:*</u>

i. Baba teaches:

(1) a plurality of centers that generate secret keys peculiar to said entities using pieces of information resulting from division of information specifying each of said entities and that sends said secret keys to said entities **[i.e., referring to Figure 3, generating, in the center, that could be a plurality of centers (see column16, line 8) , a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by the center only and common to the entities and which includes at least an integral transformation algorithm, and distributing, from the center, the secret private key and the integral transformation algorithm to each of the entities (column 2, lines 50-57)];** and

(2) a plurality of entities each of which generates a common key employed mutually in said encryption and decryption processing when communicating with another entity, using a component contained in own secret key sent from the centers, the component corresponding to one or more pieces of information specifying said another entity **[i.e., a method of sharing a common cryptokey for encrypting and decrypting communication data between entities in a network which includes a plurality of entities and a center, comprising the steps of generating, in the center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by the center only and common to the entities and which includes at least an integral transformation algorithm, and distributing, from the center, the secret private key and the integral transformation algorithm to each of the entities, and when the entities communicate with each other, applying, in each of the entities, the integral transformation algorithm and the secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate a common cryptokey, so that the entities will possess the common cryptokey shared by the entities (column 2, lines 46-63)].**

g. *Referring to claim 9:*

i. Baba teaches:

(1) a computer readable recording medium that stores a program that generates at entities involved in communications common keys used in processing to encrypt plaintext to ciphertext and in processing to decrypt said ciphertext to said plaintext in a cryptographic communications system, comprising: first program code means for causing said computer to select a component corresponding to one or more of divided pieces of information specifying one entity from a secret key peculiar to another entity; and second program code means for causing said computer to generate said common keys using said components selected **[i.e., as shown in Fligure 8, the computer of each of the entities 2 comprises a keyboard 4, a main unit 5 made up of a CPU, a RAM, a ROM, etc., and a data base 6 comprising a hard disk, that is "a**

computer readable recording medium", or the like for storing the secret private key xn, the identifier transformation algorithm, plaintexts such as sentences, programs (which can include "first program code and second program code"), etc., and encrypted communication texts (column 12, lines 19-25)].

h. *Referring to claim 10:*

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above, and **[i.e., as shown in Figure 3, wherein "the first divided specifying information being obtained bydividing specifying information of the ciphertext sendingentity into a plurality of blocks and the second dividedspecifying information being obtained by dividing specifying information of the ciphertext receiving entityinto a plurality of blocks" are considered to include in center algorithm, and "the common key having a structure of at least three layers and an exponent portion of the common key having a multi-layer structure' are considered to include in common cryptokey].**

i. *Referring to claim 11:*

i. Baba teaches:

(1) generating secret keys peculiar to entities using divided specifying information resulting from division of information specifying said entities into a plurality of blocks **[i.e., generating, in the center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm (which can include "using divided specifying information resulting from division of information specifying said entities into a plurality of blocks") which is held by the center only and common to the entities and which includes at least an integral transformation algorithm, and distributing, from the center, the secret private key and the integral transformation algorithm to each of the entities (column 2, lines 50-57)]**; and wherein

(2) secret key for a first block of divided specifying information has a multi-layer structure; and each of secret keys for remaining blocks of

divided specifying information has a single-layer structure **[i.e, referring to Figure 3, "a multi-layer structure and a single-layer structure" are considered to include in secret private key].**

j. *Referring to claim 12:*

i. This claim has limitations that is similar to those of claims 2 part (2) and 11, thus it is rejected with the same rationale applied against claims 2 part (2) and 11 above.

k. *Referring to claim 13:*

i. This claim has limitations that is similar to those of claims 3 and 10, thus it is rejected with the same rationale applied against claims 3 and 10 above.

l. *Referring to claim 22:*

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 5-6, 14-21, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baba (US 5,987, 129).

a. *Referring to claims 5 and 6:*

i. Baba does not explicitly teaches:

(1) wherein computation formulas for generating secret keys at said centers.

(2) wherein computation formulas for generating common keys at said entities.

ii. However, Baba does imply:

(1) as shown in Figure 3, cryptographic communications are carried out between the entities i, j after the center 1 generates and distributes the secret private key Xn in a preparatory stage. In the preparatory stage, the center 1 generates a center algorithm, that is "computation formulas", which serves as a basis for generating the secret private key Xn of each entity when the center 1 is established or the cryptosystem is updated (step 1) **(column 7, lines 62-67 through column 8, lines 1-2).**

(2) referring back to Figure 3, when the entities 2 (i, j, . . .) are subscribed to the cryptosystem, the center 1 generates a secret private key Xn peculiar to each of the entities 2 and an identifier transformation algorithm, that is "computation formulas" for generating a common cryptokey Kij **(column 8, lines 66-67 through column 9, lines 1-3)].**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) fully define by an expression containing mathematical function/formulas as in the center algorithm and identifier transformation algorithm of Baba.

iv. The ordinary skilled person would have been motivated to:

(1) fully reveal or express containing mathematical function/formulas about the generation of secret key and common key as shown in Figure 3 of Baba, a flowchart of an operation sequence of the cryptosystem shown in Figure 1 of Baba.

b. *Referring to claim 14:*

i. This claim has limitations that is similar to those of claims 5 and 10, thus it is rejected with the same rationale applied against claims 5 and 10 above.

c. *Referring to claim 15:*

i. This claim has limitations that is similar to those of claims 5 and 12, thus it is rejected with the same rationale applied against claims 5 and 12 above.

d. *Referring to claims 16 and 18:*

i. These claims have limitations that is similar to those of claim 6, thus they are rejected with the same rationale applied against claim 6 above.

e. *Referring to claim 17:*

i. This claim has limitations that is similar to those of claims 3 and 5, thus it is rejected with the same rationale applied against claims 3 and 5 above.

f. *Referring to claim 19:*

i. Baba teaches:

(1) a common key generator provided at entities in a cryptographic communications system for generating a common key to be used in processing to encrypt plaintext to ciphertext and in processing to decrypt ciphertext back to plaintext **[i.e., referring to Figure 8, the main unit 5 includes as its functions a common key generator 7 for generating a common key, an encrypting and decrypting processor 8 for encrypting and decrypting communication data (column 12, lines 25-28)]**, comprising:

(2) This claim also has limitations that is similar to those of claims 6 and 7, thus it is rejected with the same rationale applied against claims 6 and 7 above.

g. *Referring to claim 20:*

i. This claim has limitations that is similar to those of claims 6, 8, and 10, thus it is rejected with the same rationale applied against claims 6, 8, and 10 above.

h. *Referring to claim 21:*

i. This claim has limitations that is similar to those of claims 6, 9, and 10, thus it is rejected with the same rationale applied against claims 6, 9, and 10 above.

i. *Referring to claim 23:*

i. This claim has limitations that is similar to those of claims 6 and 9, thus it is rejected with the same rationale applied against claims 6 and 9 above.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Baba (US 5, 987, 128) discloses a method for effecting cryptographic communications between entities i, j using a common cryptokey, each of the entities i, j generates a common cryptokey by applying an identifier transformation algorithm and a secret private key, which have previously been distributed from a center, to the identifier of the other entity with which to communicate (step 3) (see abstract).

b. Greenberg (US 5,220, 606) discloses a cryptographic communications system and method. The system includes a communications channel that is coupled to an encryption device and to a decryption device (see abstract).

c. Bellovin et al (US 5, 241, 599) discloses A cryptographic communication system. The system, which employs a novel combination of public and private key cryptography, allows two parties, who share only a relatively insecure password, to bootstrap a computationally secure cryptographic system over an insecure network (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT

February 9, 2004

[illegible]
PRIMARY PATENT EXAMINER
TECHNOLOGY CENTER 2100